



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/673,137	10/11/2000	Denis Pinkas	T2147-906620	9518
181	7590	08/30/2004	EXAMINER	
MILES & STOCKBRIDGE PC 1751 PINNACLE DRIVE SUITE 500 MCLEAN, VA 22102-3833			DINH, MINH	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 08/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

<b>Application No.</b> 09/673,137  <b>Examiner</b> Minh Dinh	<b>Applicant(s)</b> PINKAS, DENIS
<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM

### THE MAILING DATE OF THIS COMMUNICATION.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.

If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.

If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) Responsive to communication(s) filed on \_\_\_\_.  
 2a) This action is FINAL.      2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) Claim(s) 7-12 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_ is/are allowed.  
 6) Claim(s) 7-12 is/are rejected.  
 7) Claim(s) \_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 11 October 2000 is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
     1. Certified copies of the priority documents have been received.  
     2. Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
     3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
     Paper No(s)/Mail Date 10/11/2000
- 4) Interview Summary (PTO-413)  
     Paper No(s)/Mail Date. \_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_.

Application/Control Number: 09/673,137  
Art Unit: 2132

## DETAILED ACTION

1. Claims 7-12 have been examined.

### *Oath/Declaration*

2. The declaration is objected to because it contains an entry (PCT application) with a date (filing date of 10/02/2000) later than that of the applicant's signature (04/05/1999). Applicant is required to provide either an explanation of the time discrepancy or a new declaration.

### *Drawings*

3. The drawings are objected to because: French words are used in figure 1 (element 18) and figure 2b (step 1004b); they need to be translated into English. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in

Application/Control Number: 09/673,137

Art Unit: 2132

the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

4. The abstract of the disclosure is objected to because it contains more than 150 words and one paragraph. Correction is required. See MPEP § 608.01(b).
  
5. The disclosure is objected to because of the following informalities:
  - a. The phrase "request to certify a public key derived from a pair of asymmetric keys, a public key K<sub>p</sub> and a private key K<sub>s</sub>" (specification page 2, lines 22-23; page 7, lines 9-10). The public key sent to the CA to be certified (page 3, lines 12-13) is not derived from an asymmetric key pair; it is the public key K<sub>p</sub> of the asymmetric key pair.
  - b. There is no brief description for figure 4c.Appropriate correction is required.

### ***Claim Objections***

6. Claims 7 and 12 are objected to because of the following informalities:
  - a. Regarding claim 7, the phrase "verifying the usage of public keys derived from a set of asymmetric keys, a public key K<sub>p</sub> and private key K<sub>s</sub>" in the preamble (1<sup>st</sup>-2<sup>nd</sup> lines). The public key sent to the CA to be verified (25<sup>th</sup>-27<sup>th</sup> lines) is not derived from

Application/Control Number: 09/673,137

Art Unit: 2132

an asymmetric key pair; it is the public key K<sub>p</sub> of the asymmetric key set. Appropriate correction is required. The phrase is interpreted as "verifying the usage of the public key of an asymmetric key pair, a public key K<sub>p</sub> and a private key K<sub>s</sub>".

b. Regarding claim 7, the phrase "by an on-board system and stored in the storage area of an on-board system (S<sub>i</sub>)" (3<sup>rd</sup>-4<sup>th</sup> lines). Since the key pair is generated by and stored on the same on-board system, the phrase is interpreted as "by an on-board system (S<sub>i</sub>) and stored in the storage area of said on-board system (S<sub>i</sub>)".

c. Regarding claim 7, the phrase "publishing said mother private key (K<sub>pM</sub>)" (17<sup>th</sup> line). It should be changed to "publishing said mother public key (K<sub>pM</sub>)".

d. Regarding claim 12, "said signature of a certification request" (14<sup>th</sup>-15<sup>th</sup> lines) should be changed to "said signature of the certification request"

#### ***Claim Rejections - 35 USC § 112***

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 7-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

a. Regarding claims 7 and 12, both claim contain the feature of calculating a diversified private key from a mother private key and a serial/identification number (claim 7: lines 20-22; claim 12: lines 5-8). According to the specification, the key diversification process implemented in step 1003, as represented in Fig. 3, can thus consist in a process supported by an algorithm known as a Zero Knowledge Signature Mechanism and the algorithms known by the names FIAT-SHAMIR or GUILLOU QUISQUATER that are usable for this purpose (lines 9-12) and a diversified private key is considered to have been obtained by implementing processes supported by the FIAT-SHAMIR algorithm F-S or the GUILLOU-QUISQUATER algorithm G-Q (lines 13-14). However, the specification fails to convey enough information to enable one skilled in the art to implement the key diversification process using the above-mentioned algorithms. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention.

b. Claims 8-11 are rejected on the same basis as claim 7 recited in paragraph 8a by virtue of their dependencies.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 7-11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Application/Control Number: 09/673,137

Art Unit: 2132

- a. Regarding claim 7, it recites the limitation "the request" in line 8<sup>th</sup>. There is insufficient antecedent basis for this limitation in the claim.
- b. Regarding claim 7, there is no indication of what value CA1 is (26<sup>th</sup> line) in the claim. The value is interpreted as an algorithm that the public key is generated to use with (specification, p. 2, lines 23-24).
- c. Claims 8-11 are rejected on the same basis as claim 7 recited in paragraphs 10a-10b by virtue of their dependencies.

***Claim Rejections - 35 USC § 103***

11. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas et al. (5,164,988) over Pauschinger (6,041,704), Austin (4,944,007) and Yuval et al. (5,586,186).

- a. Regarding claim 7, Matyas discloses a method for verifying the usage of the public key of an asymmetric key pair, a public key (PUMa) and private key (PRAa) generated for a given use, such as encryption/decryption or digital signature verification/generation, by an on-board system and stored in the storage area of the on-board system (col. 5, lines 26-36; col. 19, line 56 – col. 20, line 4) equipped with cryptographic calculation means and externally accessible read/write-protected means for storing digital data (fig. 3), said digital data comprising at least a device ID for identifying the on-board system (fig. 4, element 119), a request being formulated by said on-board system by transmitting a request message containing said public key (PUMa) to a certification (authority) (CA) (fig. 7), comprising:

Application/Control Number: 09/673,137

Art Unit: 2132

calculating for said on-board system a public and private authentication keys (PUAa and PRAa) and storing the authentication keys in said storage area (col. 17, line 65 – col. 18, line 15); publishing said public authentication key (PUAa) and said device ID (col. 18, lines 32-34); generating by the on-board system a certification request containing the public key (PUMa), an algorithm that the public key is generated to use with, and usage indicators (U) of said public key (figures 6-7; col. 5, lines 26-36); using said calculation means and said private authentication key associated with this on-board system (PRAa) to calculate a digital signature of the entire request (col. 16, lines 19-25); forming a certification request message containing the request, the identifier of the on-board system and the digital signature of the request (fig. 7; col. 16, lines 19-25); retrieving, from the certification request message, the device ID of the on-board system (col. 21, line 67 – col. 22, line 25); retrieving, from said device ID, the public authentication key (PUAa) of the on-board system, verifying, from said public authentication key (PUAa), from said device ID of the on-board system, and from said certification request message received, said digital signature, and establishing the authenticity of said cryptographic control value and the source of this certification request (fig. 5; col. 21, line 67 – col. 22, line 25; fig. 5).

Matyas does not disclose associating an identification code of an authorized operator with the on-board system. Pauschinger discloses associating a manufacture ID of a security device, which meets the limitation of an identification code of an authorized operator, with the security device (col. 7, lines 10-12; col. 8, lines 58-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Matyas method to associating the on-board system with the manufacture ID, as taught by Pauschinger. The manufacture ID together with the device ID is used to retrieve the public key of the device.

Matyas does not disclose that the private authentication key (PRAa) is a diversified private key. Austin discloses generating a private authentication key for a smart card to perform cryptographic functions, the private authentication key being a diversified private key (col. 3, lines 17-33; fig. 5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Matyas method such that the private authentication key is a diversified private key, as taught by Austin. The motivation for doing so would have been to verify that any member using its diversified private key is a legitimate member of the group (col. 3, lines 50-54).

Matyas does not disclose that the diversified private key is generated from a mother private key and the device ID. Yuval discloses a method for generating mother public and private keys and generating a diversified private key for an entity from the mother private key and information unique to that entity, the diversified private key being used to decrypt data encrypted with the mother public key (figures 5A-5C). It would have been obvious to one of ordinary skill in the art at the time the invention was

made to modify the method of Matyas further such that the diversified private key is generated from a mother private key and information unique to the on-board system, as taught by Yuval; accordingly, the unique information being the device ID. The motivation for doing so would have been that software encrypted using a single encryption key could be decrypted using multiple decryption keys, each of which is unique to a particular user (col. 2, lines 64-67).

b. Claim 8 is rejected on the same basis as claim 7.

12. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Pauschinger, Austin and Yuval as applied to claim 7 above, and further in view of Multerer et al. (6,134,658). Matyas, Pauschinger, Austin and Yuval do not disclose the steps of communicating a certification request template to said on-board system; at the on-board system level, verifying the format of the template and filling in missing fields of the certification request template. Multerer discloses automating the certification request process by communicating a certification request template to an entity requesting a certificate, verifying the format of the template and filling in missing fields of the certification request template by the entity (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Matyas, Pauschinger, Austin and Yuval to communicate a certification request template to said on-board system; at the on-board system level, verifying the format of the template and filling in missing fields of the certification request

template, as taught by Multerer, in order to minimize the number of malformed authentication certificate requests (Abstract).

13. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Pauschinger, Austin and Yuval as applied to claim 7 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography"). Matyas, Pauschinger, Austin and Yuval do not disclose controlling the asymmetric keys for only signature generation purposes. Menezes discloses controlling asymmetric keys for singing only (p. 567, 13.32 Remark). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Matyas, Pauschinger, Austin and Yuval such that the asymmetric keys is controlled for singing purposes only, as taught by Menezes. The reason for separation is that asymmetric encryption keys and signature keys have different life cycle requirements and cryptographic prudence.

14. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Pauschinger, Austin and Yuval as applied to claim 7 above, and further in view of Holloway ("Controlling The Use Of Cryptographic Keys"). Matyas, Pauschinger, Austin and Yuval do not disclose associating, with an asymmetric key pair and with the asymmetric decryption process, a symmetric weak decryption process and key, the symmetric decryption key being encrypted, then decrypted, by means of the private asymmetric decryption key. Holloway discloses controlling an asymmetric key pair for encrypting/decrypting a symmetric key (p. 597, see Hybrid Public-Symmetric Control).

Art Unit: 2132

Holloway also disclose controlling the use of weak symmetric keys (p. 594, "The base control vector ... sent encrypted to another system"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Matyas, Pauschinger, Austin and Yuval to control an asymmetric key pair for encrypting/decrypting a symmetric key, as taught by Holloway, to provide only one bridge between the asymmetric cryptographic system and the symmetric system. Also, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Matyas, Pauschinger, Austin and Yuval to control the use of weak symmetric keys, as taught by Holloway, for export control.

15. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas over Austin and Yuval. Matyas discloses:

an on-board system comprising a card having a microprocessor, a RAM, a nonvolatile memory including a programmable memory and an externally accessible protected storage area memory, a cryptographic calculation module and an input/output system connected by a link of BUS type (fig. 3)

a private authentication key (PRAa) and a corresponding public authentication key (PUAa) stored in said protected memory (fig. 4);

said cryptographic calculation module comprising:

means for calculating a signature from said private authentication key, making it possible to calculate the signature of a certification request to certify a public key PUMa associated with a private encryption key PRMa, said private key PRMa

generated by said signature calculation means being stored in said externally accessible protected memory, said signature of the certification request being a function of the identification number of said on-board system (col. 16, lines 10-25; col. 19, line 56 – col. 20, line 4; col. 3, lines 34-39), said signature calculation means making it possible to transmit to a certification authority a certification request message containing said certification request and said signature (col. 16, lines 10-25), which allows said certification authority to verify the source of the certification request from said on-board system and the protection of said private authentication key and private encryption key in said externally accessible protected memory using only public elements, such as said public authentication key PUAa (fig. 10).

Matyas does not disclose that the private authentication key (PRAa) is a diversified private key. Austin discloses generating a private authentication key for a smart card to perform cryptographic functions, the private authentication key being a diversified private key (col. 3, lines 17-33; fig. 5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Matyas method such that the private authentication key is a diversified private key, as taught by Austin. The motivation for doing so would have been to verify that any member using its diversified private key is a legitimate member of the group (col. 3, lines 50-54).

Matyas does not disclose that the diversified private key is generated from a mother private key and the device ID. Yuval discloses a method for generating mother public and private keys and generating a diversified private key for an entity from the mother private key and information unique to that entity, the diversified private key being

Art Unit: 2132

used to decrypt data encrypted with the mother public key (figures 5A-5C). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas further such that the diversified private key is generated from a mother private key and information unique to the on-board system, as taught by Yuval; accordingly, the unique information being the device ID. The motivation for doing so would have been that software encrypted using a single encryption key could be decrypted using multiple decryption keys, each of which is unique to a particular user (col. 2, lines 64-67).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/673,137  
Art Unit: 2132

Page 14

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
8/26 /04

*Gilberto Barron*  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100